I. POLICY STATEMENT

Prevention of unauthorized access to UMass Lowell’s restricted and/or confidential information, will be maintained by controlling the use, re-use, storage and disposal of media containing such information.

The surplus, transfer, trade-in, disposal of computers, or replacement of electronic storage media, and computer software can create information security risks for the University. This also includes equipment reassigned, or released, or no longer in use in the University. Failure to properly purge data in these circumstances may result in unauthorized access to University data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

II. PURPOSE

The purpose of this policy is to protect University data from unauthorized disclosure. This policy defines the requirements for ensuring University data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools - even data from files that were deleted long ago or a hard drive that was reformatted.

III. SCOPE

This policy applies to all university colleges, departments, and administrative units that utilize computer-related hardware and software that store University data.

IV. DEFINITIONS

DeGaussing
Demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.
Disintegration
A physically destructive method of sanitizing data; the act of separating into component parts.

HIPAA
Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.

Incineration
A physically destructive method of sanitizing media; the act of burning completely to ashes.

Internal Data
University Data intended for internal University business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. See UMass Lowell Data Classification Policy for an expanded definition and examples.

Media
Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.

Media sanitization
The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

Public Data
University Data explicitly or implicitly approved for distribution to the public without restriction. See UMass Lowell Data Classification Policy for an expanded definition and examples.

Pulverization
A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

Purging
A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

University Data
Any data related to UMass Lowell ("University") functions that are a) stored on University information technology systems, b) maintained by UMass Lowell faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

V. PROCEDURES
While the primary purpose of this policy is to protect non-public University Data (e.g., data classified either restricted or confidential), it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient and cost effective to purge all University data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.
Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside the University, all University data must be purged from the media before giving it to the third party.

Specific instructions for different types of media and regulations:

A. **Electronic Storage Media** (hard disk drives in computers, copiers, external hard drives, USB flash drives, magnetic tapes, etc.)

1) If purging is done by overwriting the data, the entire media/device must be overwritten with a minimum of three passes.
2) Equipment that can store University data, such as desktop/laptop computers, copiers, or external hard drives, and is permanently leaving the control of the University should have all data storage devices removed before disposition. If the equipment leaving University control must retain the data storage devices, all University Data must be properly purged.
3) The acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, hole punching, or incineration.
4) Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.

B. **Paper-Based Media**

1) Any paper-based or other hard copy media containing confidential University Data must be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by the University for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (1/32"x1/5"). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the institution, an affiliated organization, or an individual. The maximum particle size for media containing internal data is 2x15 mm (1/16"x3/5").
2) Incineration and/or recycling by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

C. **Optical Media** (e.g., CDs and DVDs)

Optical media containing restricted and confidential University data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

D. **Smartphones and Tablets**

Mobile devices such as tablets, smartphones, and even cell phones store information and often contain personal or other sensitive information. Any University data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.
E. Other Media Types

For other media and additional guidelines, refer to NIST Special Publication 800-88, Revision1: Guidelines for Media Sanitization, Appendix A, Minimum Sanitization Recommendations.

F. Export Controls

Media containing University data in equipment that will be reused outside the United States must comply with export laws and regulations according to the University’s Export Control Program through the Office of Institutional Research.

G. Electronic Protected Health Information

UMass Lowell departments responsible for electronic protected health information covered by HIPAA must also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, Physical Safeguards, part (d), (1) & (2).

H. Federal Tax Information

UMass Lowell departments handling Federal Tax Information must also have media sanitization and disposal policies and procedures in accordance with IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies.

I. Asset Management/Inventory Control

All dispositioned equipment must follow established UMass Lowell Procurement procedures and/or policies for asset management and inventory control.

J. Operational Responsible Organizations

Questions pertaining to the operational and/or procedural aspects of this policy can be directed to the Information Technology organization and/or Information Security organization by contacting the IT Service Desk at 978-934-4357 or emailing helpdesk@uml.edu.

VI. RESPONSIBILITY

Information Technology is the responsible organization for implementing the provisions of this policy. The University’s Chief Information Officer and the Information Security Officer are the designated point of contacts.

VII. ATTACHMENTS

None
VIII. RELATED POLICIES, PROCEDURES AND ANNOUNCEMENTS

Information Security Policy, IT-5-111 (reserved)
Data Classification Policy, IT-5-106 (reserved)

IX. APPROVAL AND EFFECTIVE DATE

On file with the Policy Office.